

## Adv DevOps Exp 10

**Aim:** To perform Port, Service monitoring, Windows/Linux server monitoring using Nagios.

### Monitoring Using Nagios:

**Step 1:** To Confirm Nagios is running on the server side Perform the following command on your Amazon Linux Machine (Nagios-host).

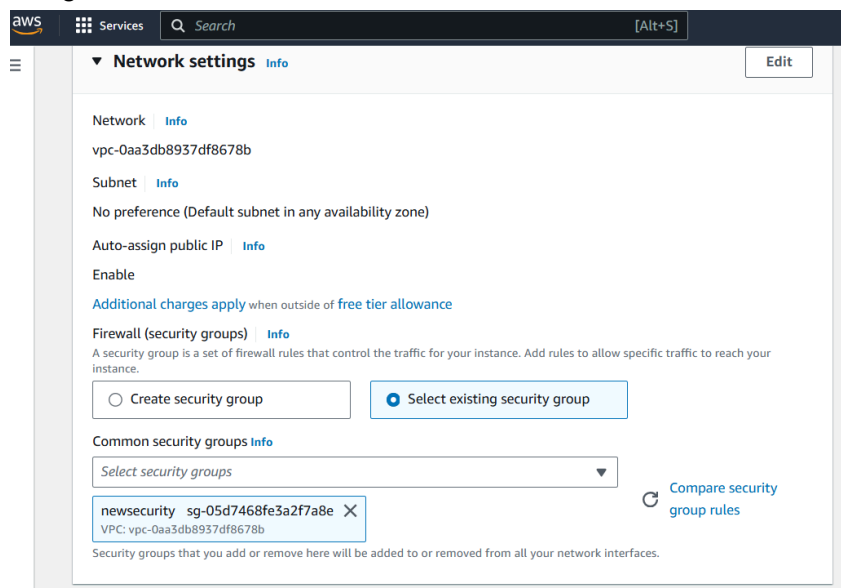
Run this command **sudo systemctl status**

```
ec2-user@ip-172-31-41-160:~/downloads/nagios-plugins-2.4.11
[ec2-user@ip-172-31-41-160 nagios-plugins-2.4.11]$ sudo systemctl status
ip-172-31-41-160.ec2.internal
State: running
Units: 296 loaded (incl. loaded aliases)
Jobs: 0 queued
Failed: 0 units
Since: Wed 2024-10-02 12:28:05 UTC; 33min ago
systemd: 252.23-2.amzn2023
CGroup: /
└─init.scope
   └─1 /usr/lib/systemd/systemd --switched-root --system --deserialize=32
      └─system.slice
         └─acpid.service
            └─1938 /usr/bin/systemd-inhibit --what=handle-suspend-key:handle-hibernate-key --who=noah "--why=acpid instead" --mode=block /usr/sbin/acpid -f
            └─2059 /usr/sbin/acpid -f
            └─amazon-ssm-agent.service
               └─7141 /usr/bin/amazon-ssm-agent
            └─atd.service
               └─2152 /usr/sbin/atd -f
            └─auditd.service
               └─1768 /sbin/auditd
            └─chronyd.service
               └─2175 /usr/sbin/chronyd -F 2
            └─dbus-broker.service
               └─1946 /usr/bin/dbus-broker-launch --scope system --audit
               └─1954 dbus-broker --log 4 --controller 9 --machine-id ec2e4d759a3e2f6fe850b14e4cdacabe --max-bytes 536870912 --max-fds 4096 --max-matches 16384 --audit
            └─gssproxy.service
               └─1959 /usr/sbin/gssproxy -D
            └─httpd.service
               └─49553 /usr/sbin/httpd -DFOREGROUND
               └─49555 /usr/sbin/httpd -DFOREGROUND
               └─49556 /usr/sbin/httpd -DFOREGROUND
               └─49557 /usr/sbin/httpd -DFOREGROUND
               └─49558 /usr/sbin/httpd -DFOREGROUND
               └─62800 /usr/sbin/httpd -DFOREGROUND
            └─libstoragemgmt.service
               └─1040 /usr/bin/lsm -d
```

**Step 2:** Before we begin,

To monitor a Linux machine, create an **Ubuntu 20.04 server** EC2 Instance in AWS.

Provide it with the **same security group** as the Nagios Host and name it 'nagios-client' alongside the host.



▼

Key pair (login)

Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

▼

[Create new key pair](#)

The screenshot shows the AWS Management Console 'Instances' page. It displays two running EC2 instances: 'nagios-host' and 'nagios-client'. Both are t2.micro instances in the us-east-1a availability zone. The 'nagios-host' instance has a public IP of ec2-34-229-45-75 and the 'nagios-client' has a public IP of ec2-54-172-92-22. Both instances show '2/2 checks passed' in the status check column.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
nagios-host	i-03facef442a77494d	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	ec2-34-229-45-75
nagios-client	i-0b934b61f21351c1b	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	ec2-54-172-92-22

### Step 3: TO BE DONE IN THE Nagios-host TERMINAL

In the nagios-host terminal, run this command

**ps -ef | grep nagios**

```
[ec2-user@ip-172-31-41-160 nagios-plugins-2.4.11]$ ps -ef | grep nagios
ec2-user  63115    2315    0 13:03 pts/0    00:00:00 grep --color=auto nagios
[ec2-user@ip-172-31-41-160 nagios-plugins-2.4.11]$
```

To become a root user, run '**sudo su**' and make two directories using the following commands. If one is running these commands in windows powershell, make sure that he/she copies it line by line as powershell might make an error while interpreting multiple lines

**mkdir /usr/local/nagios/etc/objects/monitorhosts**

**mkdir /usr/local/nagios/etc/objects/monitorhosts/linuxhosts**

```
[ec2-user@ip-172-31-92-249 ~]$ sudo su
[root@ip-172-31-92-249 ec2-user]# mkdir /usr/local/nagios/etc/objects/monitorhosts
[root@ip-172-31-92-249 ec2-user]# mkdir /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
[root@ip-172-31-92-249 ec2-user]#
```

Copy the sample localhost.cfg file to linuxhost folder. Use the following mentioned command to achieve it

**cp /usr/local/nagios/etc/objects/localhost.cfg**

**/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg**

Open linuxserver.cfg using nano and make the following changes. This is a conf type file in which we will have to modify the configurations in way which will help us specify the hosts and clients to be monitored

**nano /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg**

**Changes to be made:**

1. Change the hostname to linux-server (EVERYWHERE ON THE FILE)
2. Change address to the public IP address of your LINUX CLIENT.
3. Change hostgroup\_name under hostgroup to linux-servers1

```
# HOST DEFINITION
#
#####

# Define a host for the local machine

define host {

    use                linux-server          ; Name of host template to use
                                           ; This host definition will inherit all variables that are defined
                                           ; in (or inherited by) the linux-server host template definition.

    host_name          linux-server
    alias              localhost
    address             54.172.92.226
}
```

```
# Define an optional hostgroup for Linux machines

define hostgroup {

    hostgroup_name     linux-servers1       ; The name of the hostgroup
    alias              Linux Servers        ; Long name of the group
    members             localhost           ; Comma separated list of hosts that belong to this group
}
```

**IMP: Everywhere else on the file, change the hostname to linux-server instead of localhost.**

Open the Nagios Config file and add the following line

**nano /usr/local/nagios/etc/nagios.cfg**

Add the following line in the file and save

**cfg\_dir=/usr/local/nagios/etc/objects/monitorhosts/**

```
# OBJECT CONFIGURATION FILE(S)
# These are the object configuration files in which you define hosts,
# host groups, contacts, contact groups, services, etc.
# You can split your object definitions across several config files
# if you wish (as shown below), or keep them all in a single config file.

# You can specify individual object config files as shown below:
cfg_file=/usr/local/nagios/etc/objects/commands.cfg
cfg_file=/usr/local/nagios/etc/objects/contacts.cfg
cfg_file=/usr/local/nagios/etc/objects/timeperiods.cfg
cfg_file=/usr/local/nagios/etc/objects/templates.cfg

# Definitions for monitoring the local (Linux) host
cfg_file=/usr/local/nagios/etc/objects/localhost.cfg
cfg_dir=/usr/local/nagios/etc/objects/monitorhosts/
# Definitions for monitoring a Windows machine
#cfg_file=/usr/local/nagios/etc/objects/windows.cfg
```

Verify the configuration files by running the following command

**/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg**

```
[root@ip-172-31-41-160 nagios-plugins-2.4.11]# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

Nagios Core 4.5.5
Copyright (c) 2009-present Nagios Core Development Team and Community Contributors
Copyright (c) 1999-2009 Ethan Galstad
Last Modified: 2024-09-17
License: GPL

Website: https://www.nagios.org
Reading configuration data...
  Read main config file okay...
  Read object config files okay...

Running pre-flight check on configuration data...

Checking objects...
  Checked 16 services.
  Checked 2 hosts.
  Checked 2 host groups.
  Checked 0 service groups.
  Checked 1 contacts.
  Checked 1 contact groups.
  Checked 24 commands.
  Checked 5 time periods.
  Checked 0 host escalations.
  Checked 0 service escalations.

Checking for circular paths...
  Checked 2 hosts
  Checked 0 service dependencies
  Checked 0 host dependencies
  Checked 5 timeperiods

Checking global event handlers...
Checking obsessive compulsive processor commands...
Checking misc settings...

Total Warnings: 0
Total Errors: 0

Things look okay - No serious problems were detected during the pre-flight check
[root@ip-172-31-41-160 nagios-plugins-2.4.11]#
```

You are good to go if there are no errors.

Restart the nagios service

**service nagios restart**

And by running `sudo systemctl status nagios`, we can again check whether our server is running or not

```

root@ip-172-31-41-160:/tmp/nagios-plugins-2.4.11
[root@ip-172-31-41-160 nagios-plugins-2.4.11]# sudo systemctl restart nagios
[root@ip-172-31-41-160 nagios-plugins-2.4.11]# sudo systemctl status nagios
● nagios.service - Nagios Core 4.5.5
   Loaded: loaded (/usr/lib/systemd/system/nagios.service; enabled; preset: disabled)
   Active: active (running) since Wed 2024-10-02 13:20:17 UTC; 7s ago
     Docs: https://www.nagios.org/documentation
   Process: 78776 ExecStartPre=/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
   Process: 78777 ExecStart=/usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
   Main PID: 78778 (nagios)
    Tasks: 6 (limit: 1112)
   Memory: 4.0M
     CPU: 24ms
   CGroup: /system.slice/nagios.service
           └─78778 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
             └─78779 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             └─78780 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             └─78781 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             └─78782 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             └─78783 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Oct 02 13:20:17 ip-172-31-41-160.ec2.internal nagios[78778]: qh: echo service query handler registered
Oct 02 13:20:17 ip-172-31-41-160.ec2.internal nagios[78778]: qh: help for the query handler registered
Oct 02 13:20:17 ip-172-31-41-160.ec2.internal nagios[78778]: wproc: Successfully registered manager as @wproc with query handler
Oct 02 13:20:17 ip-172-31-41-160.ec2.internal nagios[78778]: wproc: Registry request: name=Core Worker 78782;pid=78782
Oct 02 13:20:17 ip-172-31-41-160.ec2.internal nagios[78778]: wproc: Registry request: name=Core Worker 78781;pid=78781
Oct 02 13:20:17 ip-172-31-41-160.ec2.internal nagios[78778]: wproc: Registry request: name=Core Worker 78780;pid=78780
Oct 02 13:20:17 ip-172-31-41-160.ec2.internal nagios[78778]: wproc: Registry request: name=Core Worker 78779;pid=78779
Oct 02 13:20:17 ip-172-31-41-160.ec2.internal nagios[78778]: Successfully launched command file worker with pid 78783
Oct 02 13:20:21 ip-172-31-41-160.ec2.internal nagios[78778]: HOST ALERT: linux-server;UP;SOFT;1;PING OK - Packet loss = 0%, RTA = 0.93 ms
Oct 02 13:20:24 ip-172-31-41-160.ec2.internal nagios[78778]: SERVICE ALERT: localhost;HTTP;WARNING;HARD;4;HTTP WARNING: HTTP/1.1 403 Forbidden - 319 bytes in 0.0
[root@ip-172-31-41-160 nagios-plugins-2.4.11]# sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
   Drop-In: /usr/lib/systemd/system/httpd.service.d
            └─php-fpm.conf
   Active: active (running) since Wed 2024-10-02 12:47:56 UTC; 33min ago
     Docs: man:httpd.service(8)
   Main PID: 49553 (httpd)
   Status: "Total requests: 26; Idle/Busy workers 100/0;Requests/sec: 0.0129; Bytes served/sec: 94 B/sec"
    Tasks: 238 (limit: 1112)
   Memory: 21.7M
     CPU: 1.416s
   CGroup: /system.slice/httpd.service
           └─49553 /usr/sbin/httpd -fpmctlcompmgm

```

## Step 4: TO BE DONE IN THE Nagios-client TERMINAL

Now it is time to switch to the client machine.

SSH into the machine or simply use the EC2 Instance Connect feature.

```

PS C:\WINDOWS\system32> cd C:\Users\Bell\Downloads
PS C:\Users\Bell\Downloads> ssh -i "mohit.pem" ubuntu@ec2-54-172-92-226.compute-1.amazonaws.com
The authenticity of host 'ec2-54-172-92-226.compute-1.amazonaws.com (54.172.92.226)' can't be established.
ECDSA key fingerprint is SHA256:e/WkFQRuHSqPjqQ5hDMAA0dku8msNHEtN9SAgzEy53E.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-54-172-92-226.compute-1.amazonaws.com,54.172.92.226' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1016-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Wed Oct  2 13:26:11 UTC 2024

System load:  0.0          Processes:      104
Usage of /:   22.8% of 6.71GB Users logged in:   0
Memory usage: 20%         IPv4 address for enx0: 172.31.36.100
Swap usage:   0%

 * Ubuntu Pro delivers the most comprehensive open source security and
   compliance features.

   https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by

```

Make a package index update and install gcc, nagios-nrpe-server and the plugins. Run the following commands to achieve the same.

**sudo apt update -y**

**sudo apt install gcc -y**

**sudo apt install -y nagios-nrpe-server nagios-plugins**

```
root@ubuntu172-31-36-100:~#  
root@ubuntu172-31-36-100:~# sudo apt install gcc -y  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
  
The following additional packages will be installed:  
binutils binutils-x86-64-linux-gnu cpp cpp-13 cpp-13-x86-64-linux-gnu gcc-x86-64-linux-gnu fontconfig.config fonts-dejavu-core fonts-dejavu-mono gcc-13 gcc-13-base  
gcc-13-x86-64-linux-gnu libasan5 libatomic1 libbinutils libbrotli-dev bin libbsd-dev libbz2-dev libc-devtools libc6-dev libc6-i386 libcc1-0 libcrypt-dev libcrt-nobfd libcrtf  
libdwarf2 libfontconfig1 libgcc-13-dev libgdbm3 libgomp1 libhogweed libiberty-plugin-aomdec libiberty-plugin-aomenc libiberty-plugin-libde265 libiberty-plugin-liblto libiberty  
libjpeg-turbo libjpeg8 liblerc4 liblsan5 libmpc3 libquadmath0 libstdc++6 libstdc++6-10 libtiff6 libubsan1 libwebp libxpm4 linux-libc-dev manpages-dev rpcsvc-proto  
Suggested packages:  
binutils-doc gprofng-gui gcc-13-doc gcc-13-localize gcc-13-doc-multilib make autoconf automake libtool flex bison gdc gcc-13-multilib gcc-13-doc gcc-x86-64-linux-gnu glibc-doc  
libbfd2 libffi3 libgfortran3 libgmp-dev libgnat-13 libgnat-13-dev libgnat-13-doc libgnat-13-manual libgnat-13-testsuite libgnat-13-testsuite-manual libgnat-13-testsuite-manual  
libiberty-plugin-avif libiberty-plugin-jpegdec libiberty-plugin-jpegenc libiberty-plugin-jkdec libiberty-plugin-jkenc libiberty-plugin-ravie  
libiberty-plugin-simdjit  
The following NEW packages will be installed:  
binutils binutils-common binutils-x86-64-linux-gnu cpp cpp-13 cpp-13-x86-64-linux-gnu gcc gcc-x86-64-linux-gnu fontconfig.config fonts-dejavu-core fonts-dejavu-mono gcc-13 gcc-13-base  
gcc-13-x86-64-linux-gnu gcc-x86-64-linux-gnu libasan5 libatomic1 libbinutils libc-devtools libc6-dev libc6-i386 libcrypt-dev libcrt-nobfd libcrtf libdwarf2 libfontconfig1  
libgcc-13-dev libgdbm3 libgomp1 libhogweed libiberty-plugin-aomdec libiberty-plugin-aomenc libiberty-plugin-libde265 libiberty-plugin-liblto libiberty-plugin-liblto liblto  
libjpeg-turbo libjpeg8 liblerc4 liblsan5 libmpc3 libquadmath0 libstdc++6 libstdc++6-10 libtiff6 libubsan1 libwebp libxpm4 linux-libc-dev manpages-dev rpcsvc-proto  
0 upgraded, 57 newly installed, 0 to remove and 6 not upgraded.  
Need to get 62.8 MB of archives.  
After this operation, 222 MB of additional disk space will be used.  
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 binutils-common amd64 2.42-4ubuntu2 [239 kB]  
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libstdc++6 amd64 14.2.0-4ubuntu2 [418.0 kB]  
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libbinutils amd64 2.42-4ubuntu2 [572 kB]  
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libcrtf-nobfd amd64 2.42-4ubuntu2 [97.1 kB]  
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libcrtf64 amd64 2.42-4ubuntu2 [94.5 kB]  
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libgprofng0 amd64 2.42-4ubuntu2 [851 kB]  
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 binutils-x86-64-linux-gnu amd64 2.42-4ubuntu2 [2469 kB]  
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 binutils amd64 2.42-4ubuntu2 [18.0 kB]  
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 gcc-13-base amd64 13.2.0-3ubuntu4 [49.0 kB]  
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libisl23 amd64 0.26-build1 [680 kB]  
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libmpc3 amd64 1.3.1-1build1 [54.5 kB]  
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 gcc-13-x86-64-linux-gnu amd64 13.2.0-3ubuntu4 [11.2 MB]  
Get:13 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 gcc-13 amd64 13.2.0-3ubuntu4 [1032 B]  
Get:14 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 gcc-x86-64-linux-gnu amd64 4:13.2.0-7ubuntu1 [5326 B]  
Get:15 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 gcc amd64 4:13.2.0-7ubuntu1 [22.4 kB]  
Get:16 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 fonts-dejavu-mono all 2.37-8 [502 kB]  
Get:17 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 fonts-dejavu-core all 2.37-8 [835 kB]  
Get:18 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 fontconfig.config amd64 2.15.0-1ubuntu2 [37.3 kB]  
Get:19 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libecj1 amd64 14-20240412-0ubuntu1 [47.7 kB]  
Get:20 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libgomp1 amd64 14-20240412-0ubuntu1 [147 kB]  
Get:21 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libitm1 amd64 14-20240412-0ubuntu1 [28.9 kB]
```

```
root@ubuntu:/# dpkg-query -f='${Package} ${Version} ${Architecture}\n' -W -f='${Package} ${Version} ${Architecture}\n' | grep nagios-nrpe-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'monitoring-plugins' instead of 'nagios-plugins'
The following additional packages will be installed:
libavahi-client3 libavahi-common-data libavahi-common libcupscpp2 libdbus-1-3 libltdl7 libmnl0 libnss-mdns libnss-systemd libnss3-base libsmbclient6
libtalloc2 libtdb1 libtevent0t64 liburiparser1 libbsdnetmon0 monitoring-plugins-basic monitoring-plugins-common monitoring-plugins-standard mysql-common python3-gpg python3-lib
python3-random python3-samba python3-talloc python3-tdb python3-rpcbind samba-common samba-common-bin samba-dfs-modules samba-lsb smbclient snmp
Suggested packages:
cups-common libcrypt-dev perl libdigest-hmac-perl libio-socket-inet-perl snmp-mibs-downloader icinga2 nagios-plugins-contrib postfix | sendmail-bin | exim4-daemon-heavy
| exim4-daemon-light xinetd | inetd python-markdown-doc heimdal-clients python3-dnswatch cifs-utils
The following new packages will be installed:
libavahi-client3 libavahi-common-data libavahi-common libcupscpp2 libdbus-1-3 libltdl7 libmnl0 libnss-mdns libnss-systemd libnss3-base libsmbclient6
libtalloc2 libtdb1 libtevent0t64 liburiparser1 libbsdnetmon0 monitoring-plugins-basic monitoring-plugins-common monitoring-plugins-standard mysql-common
python3-gpg python3-lib python3-random python3-samba python3-talloc python3-tdb python3-rpcbind samba-common-bin samba-dfs-modules samba-lsb smbclient snmp
0 upgraded, 39 newly installed, 0 to remove and 6 not upgraded.
Need to get 16.1 MB of archives.
After this operation, 72.8 MB of additional disk space will be used.
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 nagios-nrpe-server amd64 4.1.0-1ubuntu3 [356 kB]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 rpcbind amd64 1.2.6-7ubuntu2 [46.5 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libavahi-common-data libavahi-common-data 0.8-13ubuntu6 [29.7 kB]
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libavahi-common3 amd64 0.8-13ubuntu6 [23.3 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libavahi-client3 amd64 0.8-13ubuntu6 [26.6 kB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 libcupscpp2 amd64 2.4.7-1~ubuntu3.3 [272 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libdbus-1-3 amd64 1.13.18-1ubuntu1 [46.8 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libltdl7 amd64 0.9.0-6-build1 [25.7 kB]
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libtalloc2 amd64 2.4.2-1build1 [27.3 kB]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libtdb1 amd64 1.4.10-1ubuntu1 [46.8 kB]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libtevent0t64 amd64 0.16.1-1ubuntu1 [42.6 kB]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 liburiparser1 amd64 0.9.8+samba4.19.5+dfsg-4ubuntu9 [187 kB]
Get:13 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 mysql-common all 5.8.1-1build1 [674B]
Get:14 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 libmnl0 amd64 1:1.0.5-3ubuntu2 [24.0kB]
Get:15 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libnss-mdns amd64 1:3.10.3-4ubuntu1 [206 kB]
Get:16 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 libnss-systemd amd64 2.4.0-2ubuntu2 [1294 kB]
Get:17 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libnss3-base amd64 2:4.0-1ubuntu3 [786.8 kB]
Get:18 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 libnss3 amd64 2:4.0-1ubuntu3 [786.8 kB]
Get:19 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libsmbclient6 amd64 2:4.19.5+dfsg-4ubuntu9 [6017 kB]
Get:20 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 samba-lsb amd64 2:4.19.5+dfsg-4ubuntu9 [62.4 kB]
Get:21 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libldb-base amd64 2:2.0.25+dfsg-1ubuntu1 [206 kB]
Get:22 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libldb-schema amd64 2:2.0.25+dfsg-1ubuntu1 [206 kB]
Get:23 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libldb-util amd64 2:2.0.25+dfsg-1ubuntu1 [206 kB]
Get:24 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libldb-testutils amd64 2:2.0.25+dfsg-1ubuntu1 [206 kB]
Get:25 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 python3-markdown all 3.5.2-1 [72.0 kB]
```

Open nrpe.cfg file to make changes.

**sudo nano /etc/nagios/nrpe.cfg**

Under allowed\_hosts, add your nagios host IP address like so

```
ubuntu@ip-172-31-36-100: ~
GNU nano 7.2
#
# Note: The daemon only does rudimentary checking of the client's IP
# address. I would highly recommend adding entries in your /etc/hosts.allow
# file to allow only the specified host to connect to the port
# you are running this daemon on.
#
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd
allowed_hosts=127.0.0.1,34.229.45.75
#
# COMMAND ARGUMENT PROCESSING
# This option determines whether or not the NRPE daemon will allow clients
# to specify arguments to commands that are executed. This option only works
# if the daemon was configured with the --enable-command-args configure script
```

Now restart the NRPE server by this command.

**sudo systemctl restart nagios-nrpe-server**

```
ubuntu@ip-172-31-36-100: ~
ubuntu@ip-172-31-36-100:~$ sudo systemctl restart nagios-nrpe-server
ubuntu@ip-172-31-36-100:~$
```

Run the following command in the Nagios-host terminal

**sudo systemctl status nagios**

```
[root@ip-172-31-41-160 nagios-plugins-2.4.11]# sudo systemctl status nagios
● nagios.service - nagios core 4.5.3
   Loaded: loaded (/usr/lib/systemd/system/nagios.service; enabled; preset: disabled)
   Active: active (running) since Wed 2024-10-02 13:20:17 UTC; 15min ago
     Docs: https://www.nagios.org/documentation
   Main PID: 78778 (nagios)
    Tasks: 6 (limit: 1112)
   Memory: 4.3M
      CPU: 403ms
  CGroup: /system.slice/nagios.service
          └─78778 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
             └─78779 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
                └─78780 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
                   └─78781 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
                      └─78782 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
                         └─78783 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Oct 02 13:22:54 ip-172-31-41-160.ec2.internal nagios[78778]: SERVICE NOTIFICATION: nagiosadmin;localhost;Swap Usage;CRITICAL;notify-service-by-email;SWAP CRITICAL - 0% free (0 MB out of 0
Oct 02 13:22:54 ip-172-31-41-160.ec2.internal nagios[78778]: wproc: NOTIFY job 3 from worker core Worker 78782 is a non-check helper but exited with return code 127
Oct 02 13:22:54 ip-172-31-41-160.ec2.internal nagios[78778]: wproc: host=localhost; service=Swap Usage; contact=nagiosadmin
Oct 02 13:22:54 ip-172-31-41-160.ec2.internal nagios[78778]: wproc: early timeout=0; exited ok=1; wait status=32512; error code=0;
Oct 02 13:22:54 ip-172-31-41-160.ec2.internal nagios[78778]: wproc: stderr line 01: /bin/sh; line 1: /bin/mail: No such file or directory
Oct 02 13:22:54 ip-172-31-41-160.ec2.internal nagios[78778]: wproc: stderr line 02: /usr/bin/printf: write error: Broken pipe
Oct 02 13:23:13 ip-172-31-41-160.ec2.internal nagios[78778]: SERVICE ALERT: linux-server;Total Processes;OK;HARD;1;PROCS OK: 37 processes with STATE = RSZDT
Oct 02 13:23:50 ip-172-31-41-160.ec2.internal nagios[78778]: SERVICE ALERT: linux-server;Current Load;OK;HARD;1;OK - load average: 0.01, 0.07, 0.04
Oct 02 13:24:28 ip-172-31-41-160.ec2.internal nagios[78778]: SERVICE ALERT: linux-server;Current Users;OK;HARD;1;USERS OK - 2 users currently logged in
Oct 02 13:24:46 ip-172-31-41-160.ec2.internal nagios[78778]: SERVICE ALERT: localhost;Current Users;OK;HARD;1;USERS OK - 2 users currently logged in
lines 1-26/26 (END)
```

**Step 5: Visiting your nagios server using your nagios-host ip address**

Open up your browser and look for `http://<public_ip_address_of_nagios-host>/nagios`

The screenshot shows the Nagios Core web interface. The browser address bar displays `34.229.45.75/nagios/`. The page features a sidebar on the left with navigation links under categories: General (Home, Documentation), Current Status (Tactical Overview, Map, Hosts, Services, Host Groups, Service Groups, Problems, Quick Search), and Reports (Availability, Trends, Alerts, Notifications, Event Log). The main content area displays the Nagios Core logo, a green checkmark indicating the daemon is running with PID 78778, and the version 4.5.5 as of September 17, 2024. Below this, there are sections for 'Get Started' (with links to monitoring, configuration, support, training, and certification), 'Quick Links' (to Nagios Library, Labs, Exchange, Support, and company/project pages), 'Latest News', and 'Don't Miss...'. A 'Page Tour' button is visible in the bottom right corner.

Click on Hosts.

The screenshot shows the Nagios Core web interface with the 'Hosts' page selected. The browser address bar displays `34.229.45.75/nagios/`. The sidebar on the left is the same as in the previous screenshot. The main content area displays the 'Current Network Status' (Last Updated: Wed Oct 2 13:40:35 UTC 2024, Updated every 90 seconds, Nagios Core 4.5.5 - www.nagios.org, Logged in as nagiosadmin). It includes 'Host Status Totals' (Up: 2, Down: 0, Unreachable: 0, Pending: 0) and 'Service Status Totals' (Ok: 12, Warning: 1, Unknown: 0, Critical: 3, Pending: 0). Below these are links to view service status details, status overview, status summary, and status grid for all host groups. The 'Host Status Details For All Host Groups' section shows a table with columns: Host, Status, Last Check, Duration, and Status Information. The table lists two hosts: 'linux-server' and 'localhost', both with a status of 'UP'. The 'Status Information' column shows 'PING OK - Packet loss = 0%, RTA = 0.84 ms' for 'linux-server' and 'PING OK - Packet loss = 0%, RTA = 0.04 ms' for 'localhost'. A 'Limit Results' dropdown is set to '100'. The text 'Results 1 - 2 of 2 Matching Hosts' is displayed below the table. A 'Page Tour' button is visible in the bottom right corner.

Host	Status	Last Check	Duration	Status Information
linux-server	UP	10-02-2024 13:40:17	0d 0h 20m 18s	PING OK - Packet loss = 0%, RTA = 0.84 ms
localhost	UP	10-02-2024 13:40:09	0d 0h 20m 26s	PING OK - Packet loss = 0%, RTA = 0.04 ms



Click on linux-server to view host information

The screenshot displays the Nagios web interface for the host 'linux-server'. The left sidebar contains navigation links for General, Current Status, Tactical Overview, Map, Hosts, Services, Host Groups, Service Groups, Problems, Reports, and System. The main content area is divided into several sections:

- Host Information:** Shows the host is 'localhost (linux-server)', a member of 'No hostgroups', and has an IP of '54.172.92.226'. It also displays the last update time and Nagios version.
- Host State Information:** A summary box showing the host is 'UP' (for 0d 0h 20m 39s). It includes performance data (PING OK, Packet loss = 0%, RTA = 0.84 ms), current attempt (1/10), last check time (10-02-2024 13:40:17), check type (ACTIVE), check latency (0.000 / 4.121 seconds), next scheduled active check (10-02-2024 13:45:17), last state change (10-02-2024 13:20:17), last notification (N/A), and is not flapping.
- Host Commands:** A list of commands with checkboxes to enable or disable them, such as 'Disable active checks of this host', 'Re-schedule the next check of this host', 'Submit passive check result for this host', etc.
- Host Comments:** A section to add or delete comments about the host.

The bottom of the interface shows a Windows taskbar with the date and time as 19:11 on 02-10-2024.

We can even navigate to the services section, which explicitly mentions the status, duration, checks, information about the numerous services present on our hosts

The screenshot displays the Nagios web interface for the 'Service Status Details For All Hosts'. The left sidebar is the same as the previous screenshot. The main content area shows a table of services for two hosts: 'linux-server' and 'localhost'.

Host	Service	Status	Last Check	Duration	Attempt	Status Information	
linux-server	Current Load	OK	10-02-2024 13:38:50	0d 0h 18m 19s	1/4	OK - load average: 0.00, 0.00, 0.00	
	Current Users	OK	10-02-2024 13:39:28	0d 0h 17m 41s	1/4	USERS OK - 3 users currently logged in	
	HTTP	CRITICAL	10-02-2024 13:40:05	0d 0h 27m 4s	4/4	connect to address 54.172.92.226 and port 80: Connection refused	
	PING	OK	10-02-2024 13:40:43	0d 0h 21m 26s	1/4	PING OK - Packet loss = 0%, RTA = 1.05 ms	
	Root Partition	OK	10-02-2024 13:41:20	0d 0h 20m 49s	1/4	DISK OK - free space: / 6122 MiB (75.43% inode=98%)	
	SSH	OK	10-02-2024 13:41:58	0d 0h 20m 11s	1/4	SSH OK - OpenSSH_9.6p1 Ubuntu-3ubuntu13.5 (protocol 2.0)	
	Swap Usage	CRITICAL	10-02-2024 13:37:35	0d 0h 24m 34s	4/4	SWAP CRITICAL - 0% free (0 MB out of 0 MB) - Swap is either disabled, not present, or of zero size.	
	Total Processes	OK	10-02-2024 13:38:13	0d 0h 18m 56s	1/4	PROCS OK: 38 processes with STATE = RSZDT	
	localhost	Current Load	OK	10-02-2024 13:40:09	0d 0h 22m 0s	1/4	OK - load average: 0.00, 0.00, 0.00
		Current Users	OK	10-02-2024 13:39:46	0d 0h 17m 23s	1/4	USERS OK - 3 users currently logged in
HTTP		WARNING	10-02-2024 13:40:24	0d 0h 21m 45s	4/4	HTTP WARNING: HTTP/1.1 403 Forbidden - 319 bytes in 0.001 second response time	
PING		OK	10-02-2024 13:41:01	0d 0h 21m 8s	1/4	PING OK - Packet loss = 0%, RTA = 0.04 ms	
Root Partition		OK	10-02-2024 13:41:39	0d 0h 20m 30s	1/4	DISK OK - free space: / 6122 MiB (75.43% inode=98%)	
SSH		OK	10-02-2024 13:37:16	0d 0h 19m 53s	1/4	SSH OK - OpenSSH_8.7 (protocol 2.0)	
Swap Usage		CRITICAL	10-02-2024 13:37:54	0d 0h 24m 15s	4/4	SWAP CRITICAL - 0% free (0 MB out of 0 MB) - Swap is either disabled, not present, or of zero size.	

Results 1 - 16 of 16 Matching Services

**Conclusion:** In conclusion, the experiment focused on monitoring ports, services, and a Linux server using Nagios. Through the step-by-step process, we successfully configured Nagios to monitor essential network services on the Linux server. By setting up both the Nagios host and client, we were able to track system performance, ensure service availability, and monitor key metrics like CPU and memory usage.